



# Data Breach Policy

## LEGAL AND LEGISLATION

V1.0 | July 2025

## TABLE OF CONTENTS

1.	PURPOSE .....	3
2.	WHAT IS A DATA BREACH? .....	3
3.	WHAT IS AN ELIGIBLE DATA BREACH? .....	3
4.	SCOPE .....	4
5.	AUTHORITY .....	5
6.	RELEVANT LEGISLATION AND DOCUMENTS.....	5
7.	ROLES AND RESPONSIBILITIES.....	5
8.	RESPONDING TO A DATA BREACH .....	8
9.	RECORD KEEPING AND REGISTER OF ELIGIBLE DATA BREACHES .....	10
10.	DOCUMENT INFORMATION .....	10
11.	VERSION HISTORY .....	11
	APPENDIX A: DEFINITIONS .....	12
	APPENDIX B: DATA BREACH RESPONSE .....	1

# 1. PURPOSE

The Queensland Building and Construction Commission (QBCC) is required to deal with personal information in compliance with the *Information Privacy Act 2009 (IP Act)*. Chapter 3A of the IP Act creates a mandatory notification of data breach (MNDB) scheme. The MNDB scheme imposes obligations on Queensland Government agencies, including the QBCC, to undertake the following steps where an agency knows or reasonably suspects that a data breach of the agency is an eligible data breach:

- Immediately, and continue to take all reasonable steps to:
  - Contain the data breach, and
  - Mitigate the harm caused by the data breach, and
- If there is uncertainty as to whether the data breach is eligible, assess whether there are reasonable grounds to believe the data breach is an eligible data breach of the agency within 30 days.

Section 73 of the IP Act requires Queensland Government agencies, including the QBCC, to publish on an accessible website a Data Breach Policy detailing how the agency will respond to a data breach that occurs in relation to personal information held by the agency.

This policy outlines the QBCC's approach to compliance with the MNDB scheme provisions set out in Chapter 3A of the IP Act, along with the associated Data Breach Response Plan (Plan), which underpins how the QBCC will:

- Limit the likelihood and impact of harm to individuals affected by a data breach
- Build public confidence in the QBCC's ability to respond to data breaches
- Meet legislative obligations to protect and safeguard personal information and privacy.

# 2. WHAT IS A DATA BREACH?

A 'data breach' of an agency is defined in schedule 5 of the IP Act and means either of the following to information held by the agency —

- a) unauthorised access to, or unauthorised disclosure of, information, or
- b) the loss of information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur.

An example of a data breach is where an agency identifies that an unknown party has gained unauthorised access to the agency's financial information. Upon assessment, the agency identifies that no personal information was subject to the data breach incident.

# 3. WHAT IS AN ELIGIBLE DATA BREACH?

An 'eligible data breach' of an agency is defined in section 47 as a data breach of an agency that occurs in relation to personal information held by the agency if—

- a) Both of the following apply—
  - (i). the data breach involves unauthorised access to, or unauthorised disclosure of, the personal information;

- (ii). the access or disclosure is likely to result in serious harm to an individual to whom the personal information relates, having regard to:
  1. the kind of personal information accessed, disclosed, or lost, and
  2. the sensitivity, and whether the personal information is protected by 1 or more security measures, and
  3. if the personal information is protected by 1 or more security measures—the likelihood that any of those security measures could be overcome; and
  4. the persons, or the kinds of persons, who have obtained, or who could obtain, the personal information; and
  5. the nature of the harm likely to result from the data breach; and
  6. any other relevant matter; or
- b) the data breach involves the personal information being lost in circumstances where—
  - (i). unauthorised access to, or unauthorised disclosure of, the personal information is likely to occur; and
  - (ii). If the unauthorised access to or unauthorised disclosure of the personal information were to occur, it would be likely to result in serious harm to an individual to whom the personal information relates, having regard to:
    1. the kind of personal information accessed, disclosed, or lost, and
    2. the sensitivity, and whether the personal information is protected by 1 or more security measures, and
    3. if the personal information is protected by 1 or more security measures—the likelihood that any of those security measures could be overcome; and
    4. the persons, or the kinds of persons, who have obtained, or who could obtain, the personal information; and
    5. the nature of the harm likely to result from the data breach; and
    6. any other relevant matter.

An example of an 'eligible data breach' may involve a cyber attack, where an unknown threat actor has gained unauthorised access to an agency's ICT system. The threat actor has gained access to the agency's financial information. The agency is aware that the financial information includes personal banking information and details of approximately 125 agency employees.

This personal information is the type of information that is often used by threat actors to commit identity theft and other related financial crimes. Based on these circumstances, the agency identifies that serious harm in the form of financial loss is likely for at least some (if not all) of the individuals to whom the personal information relates.

## 4. SCOPE

This policy applies to actual and suspected data breaches involving personal information.

Data breaches that do not involve personal information are managed in line with the appropriate QBCC policy or process (e.g., cyber security incident, critical incident, code of conduct, or information and records management processes).

This policy further applies to:

- Commissioner/Chief Executive Officer (**Commissioner**)
- Queensland Building and Construction Employing Office
- Statutory Office Holders
- Senior Executive Service (**SES**) or equivalent officers

- Employees of the Queensland Building and Construction Employing Office (QBCEO) who undertake work for the QBCC
- Members of the Queensland Building and Construction Board (QBC Board) and the QBC Board Committees, including the Industry Advisory Committee (IAC)
- Members of the Service Trades Council (STC) and its panels, the Service Trades Licensing Advisory Panel (STLAP) and the Notifiable Work Panel
- Individuals who are engaged as contractors, consultants, or service providers who provide services to the QBCC.

For this policy, the above individuals are collectively referred to as ‘the QBCC’s officers’.

## 5. AUTHORITY

Authority	Queensland Building & Construction Board
Document Owner	Chief Legal Officer
Date	June 2025
Version	V1.0 Release
Review Date	July 2026
Related Documents - forms and procedures	Privacy Policy Privacy Management Framework Data Breach Response Plan Data Breach Register Cyber Incident Response Plan Business Continuity Management System Manual Critical Incident Management Plan Information Security Management System (ISMS) Framework

## 6. RELEVANT LEGISLATION AND DOCUMENTS

- Chapter 3A of the IP Act
- Part IIIIC of the *Privacy Act 1988* (Cth)
- Privacy (Tax File Number) Rule 2015
- Information Security Policy (IS18:2018)
- Information Security Incident Reporting Standard
- *Public Records Act 2023*
- *Public Sector Act 2022*
- Code of Conduct for Queensland Public Service
- *Crime and Corruption Act 2001*

## 7. ROLES AND RESPONSIBILITIES

Roles and responsibilities relevant to this policy are set out in the table below.

ROLE	RESPONSIBILITIES
<b>QBCC employees (including fixed term), agency contractors and contractors</b>	<ul style="list-style-type: none"> <li>• Read the Data Breach Response Plan and understand what is expected of them.</li> <li>• Comply with the IP Act, including protecting personal information held by the QBCC from unauthorised access, disclosure, or loss.</li> <li>• Where required in accordance with this policy, immediately report a data breach or suspected data breach to the appropriate officer (this could be a supervisor, manager, senior officer, or privacy officer).</li> <li>• Respond to requests for information from and cooperate with the privacy officer and/or the Data Breach Response Team.</li> <li>• Completes mandatory privacy and information security-related training.</li> <li>• Takes all reasonable steps to contain the data breach and mitigate any harm.</li> </ul>
<b>Privacy officer (Director RTI and Privacy and members of the Privacy Team)</b>	<ul style="list-style-type: none"> <li>• Support the impacted business area in assessing the severity of a data breach involving personal information and the likelihood that a breach will result in serious harm to an individual to whom the information involved relates.</li> <li>• Escalate serious data breaches to the relevant senior officer or executive.</li> <li>• Notify (or arrange for a senior officer or executive to notify) the Information Commissioner, affected persons, where required. This includes publishing, monitoring, and reviewing the currency of public notifications of a data breach published to the QBCC website under section 53(1)(c) of the IP Act.</li> <li>• Immediately report a data breach that relates to personal information that is also a cyber security incident to the Chief Digital Information Officer, if not already reported.</li> <li>• Maintain the Register for Eligible Data Breaches.</li> <li>• Provides recommendations for data breach assessments and potential remediation actions.</li> <li>• Supports notification obligations to relevant parties under the MNDB scheme in consultation with the Data Breach Response Team.</li> <li>• Reviews, tests, and updates this policy and associated Plan.</li> <li>• Develops and implements privacy and data breach training and awareness activities for QBCC officers.</li> </ul>
<b>Manager (all QBCC Managers)</b>	<ul style="list-style-type: none"> <li>• Identify and escalate concerns within the area of responsibility that may enliven the requirements of this policy.</li> <li>• Immediately report a data breach that involves personal information that is also a cyber security incident to the Chief Digital Information Officer, if not already reported.</li> </ul>
<b>Senior Managers across the organisation</b>	<ul style="list-style-type: none"> <li>• Immediately report a data breach that involves personal information to the Privacy Team, if not already reported.</li> </ul>

ROLE	RESPONSIBILITIES
including Senior Leadership Team, Executive Director and Director roles	<ul style="list-style-type: none"> <li>• Where relevant, notify the Information Commissioner, affected persons, and others where required.</li> <li>• Implement the Data Breach Response Plan and related procedures.</li> <li>• Convene the Data Breach Response Team when appropriate.</li> <li>• Proactively lead data breach response and management to ensure compliance with this Policy and the associated Plan.</li> </ul>
Chief Executive Officer (CEO) and Commissioner	<ul style="list-style-type: none"> <li>• Liaises with the Data Breach Response Team and, where required, the QBC Board and Minister.</li> <li>• Immediately report a data breach that involves personal information to the Privacy Team, if not already reported.</li> <li>• Where relevant, notify the Information Commissioner, affected persons, and others where required.</li> <li>• Implement the Data Breach Response Plan and related procedures.</li> <li>• Convene the Data Breach Response Team when appropriate.</li> <li>• Proactively lead data breach response and management to ensure compliance with this Policy and the associated Plan.</li> </ul>
Data Breach Response Team (Members listed in the QBCC Data Breach Response Plan)	<ul style="list-style-type: none"> <li>• In line with the QBCC Data Breach Response Plan, manage a data breach that relates to personal information and that is considered likely to cause serious harm to any impacted individual or the QBCC's systems.</li> <li>• Oversee breach response efforts for eligible data breaches, including: <ul style="list-style-type: none"> <li>○ Investigating the data breach</li> <li>○ Taking steps to minimise harms</li> <li>○ Determining whether to involve internal or external parties to support the data breach response</li> <li>○ Supporting the assessment of data breaches, including determining whether breaches are notifiable under the MNDB scheme</li> <li>○ Overseeing notifications and reporting requirements</li> <li>○ Conducting a post-data breach review.</li> </ul> </li> </ul>
Impacted business area	<ul style="list-style-type: none"> <li>• Undertakes data breach response steps outlined in the Plan in conjunction with the Data Breach Response, Privacy, Digital and Information Services Teams, and/or other supporting areas.</li> <li>• Supports the Data Breach Response Team as required to meet notification requirements under the MNDB scheme.</li> </ul>
Digital and Information Services	<ul style="list-style-type: none"> <li>• Implements and maintains appropriate technical and organisational mechanisms to detect and report data breaches that occur within QBCC networks and systems.</li> <li>• Manages cyber security incidents in accordance with the QBCC Cyber Security Incident Response Plan.</li> <li>• Manages security incident notification and reporting requirements.</li> <li>• Collaborates with the Privacy Team when conducting tabletop exercises that involve the compromise of personal information.</li> </ul>

ROLE	RESPONSIBILITIES
Governance and Risk	<ul style="list-style-type: none"> <li>Supports the development and implementation of business continuity and critical incident management processes to ensure a coordinated response to a crisis event, including an eligible data breach event.</li> </ul>
Communication and Executive Services	<ul style="list-style-type: none"> <li>Liaises with the Data Breach Response Team to develop notification messages.</li> <li>Approves outgoing communication messages as required under the MNDB scheme.</li> <li>Coordinates the transmission of communications messages.</li> </ul>
Legal Services	<ul style="list-style-type: none"> <li>Provides legal advice on data breach-related matters and instances as required.</li> </ul>
Procurement	<ul style="list-style-type: none"> <li>Monitors contractor compliance with contractual information security and privacy protection requirements.</li> </ul>

## 8. RESPONDING TO A DATA BREACH

The QBCC takes the following steps to prepare and plan for data breaches.

### 8.1 STAGE 1: PREPARATION

The QBCC maintains a Data Breach Response Plan (**Plan**) that outlines clear data breach response steps as set out in [Appendix B](#) of this policy. The Plan focuses on meeting MNDB scheme obligations and reducing the impact of harm to affected individuals and the QBCC.

The Plan outlines the roles and responsibilities of the QBCC Data Breach Response Team (see [Appendix A](#) for the Data Breach Team composition), and aligns with other QBCC incident response processes, including processes to manage cyber incidents, critical incidents (business continuity management), and other organisational processes that may be relevant to data breach investigation and response (e.g., code of conduct matters).

#### TRAINING AND AWARENESS

The QBCC provides mandatory data breach and privacy training to all QBCC officers, which defines what a data breach is, outlines QBCC officer responsibilities, and provides an overview of the QBCC's approach to data breach management and response.

Targeted data breach response training supplements broader privacy and security training and awareness activities that raise cyber security awareness and educate QBCC officers of their privacy obligations under the IP Act.

### 8.2 STAGE 2: IDENTIFICATION

The QBCC implements and maintains various mechanisms to identify and report data breaches. Early detection of a data breach improves the QBCC's ability to contain a data breach and mitigate potential harms. These measures include:

- Clear and defined processes for QBCC officers to report identified data breaches

- Implementation of technical controls and monitoring services that monitor and flag unusual or unauthorised activity
- Regular audits and reviews, including periodic security reviews, audit logs, and reporting, and the implementation of data loss prevention policies.

### THIRD PARTY SERVICE PROVIDERS

Third-party risk management is a critical component of privacy management at the QBCC, as the involvement of contract service providers can significantly impact privacy and the security of QBCC information, including personal information held by the QBCC.

The QBCC takes steps to bind third-party service providers to comply with its privacy obligations under the IP Act. Further, depending on the agreement and service, contractual arrangements may include data breach provisions that require immediate notification by the service provider of any unauthorised access, use, modification, disclosure, or other misuse of personal information in connection with the contract.

### IDENTIFY AND REPORT A DATA BREACH

All QBCC officers are responsible for reporting actual or suspected data breaches. Prompt reporting of data breaches ensures the QBCC can respond quickly and ensure the QBCC can take steps to reduce negative impacts to individuals, QBCC officers, the QBCC, and other third parties involved.

**If you are aware of, or suspect, that a data breach relating to personal information has occurred, please contact the QBCC as soon as possible.**

Attention: Queensland Building and Construction Commission Privacy Team  
 Email: [privacy@qbcc.qld.gov.au](mailto:privacy@qbcc.qld.gov.au)  
 Post: GPO Box 5099  
 Brisbane QLD 4001

## 8.3 STAGE 3: CONTAINMENT AND MITIGATION

Where the QBCC knows or suspects there has been a data breach, it immediately takes, and continues to take, all reasonable steps to contain the data breach and mitigate the harm caused. While containing the data breach, the QBCC is careful to ensure that evidence of the breach is not destroyed.

## 8.4 STAGE 4: ASSESSMENT

The QBCC determines whether a data breach is an eligible data breach.

The QBCC considers the following factors when determining whether serious harm is likely:

- The kind of personal information accessed, disclosed, or lost
- The sensitivity of the personal information
- Whether the personal information is protected by one or more security measures, and if so, the likelihood that any of those security measures could be overcome

- The persons, or the kinds of persons, who have obtained, or who could obtain, the personal information
- The nature of the harm likely to result from the data breach
- Any other relevant matter.

The QBCC will complete the assessment as soon as practicable, and within 30 calendar days. If the QBCC is not able to complete the assessment within this period, it requests an extension from the Queensland Information Commissioner.

## 8.5 STAGE 5: NOTIFICATION

Where the QBCC determines that an eligible data breach has occurred, it will notify the Information Commissioner and individuals affected by the breach, unless an exemption outlined in the MNDB scheme applies.

The QBCC understands the benefits of data breach notification and does so with the intent of empowering individuals, enhancing transparency, and building trust.

Depending on the circumstances of the breach, the QBCC may also notify other organisations (such as the Australian Information Commissioner, Queensland Police Service, or the Queensland Government Information Security Virtual Response Team).

Further, where the QBCC becomes aware that a known or suspected eligible data breach may affect another agency, the QBCC will notify the agency of the data breach.

## 8.6 STAGE 6: POST-DATA-BREACH REVIEW AND REMEDIATION

The QBCC conducts a post-data breach review and evaluation to identify possible improvements to prevent similar data breaches from occurring and identifies what is needed to ensure it can proactively and effectively manage future data breaches.

# 9. RECORD KEEPING AND REGISTER OF ELIGIBLE DATA BREACHES

The QBCC maintains appropriate data breach records to provide evidence of how known and suspected data breaches are managed. This includes keeping a register of eligible data breaches of the agency, as required under section 72 of the IP Act.

# 10. DOCUMENT INFORMATION

INFORMATION CATEGORY	DESCRIPTION
Title	Data Breach Policy
Purpose	Details how the QBCC manages and responds to a data breach relating to personal information.
Document Type	Policy

Category	Right to Information and Privacy
Sub-category	Privacy
Approver	<b>Queensland Building and Construction Board</b>
Author	Director Right to Information and Privacy
Owner	Chief Legal Officer
Steward	Director Right to Information and Privacy
Version	<b>V1.0 Release</b>
Effective date	July 2025
Review date	July 2026

## 11. VERSION HISTORY

VERSION	DATE	AMENDMENT DETAILS
V0.1	June 2025	Draft version
V1.0	July 2025	Release version

# APPENDIX A: DEFINITIONS

Terms used within this policy are defined in the table below.

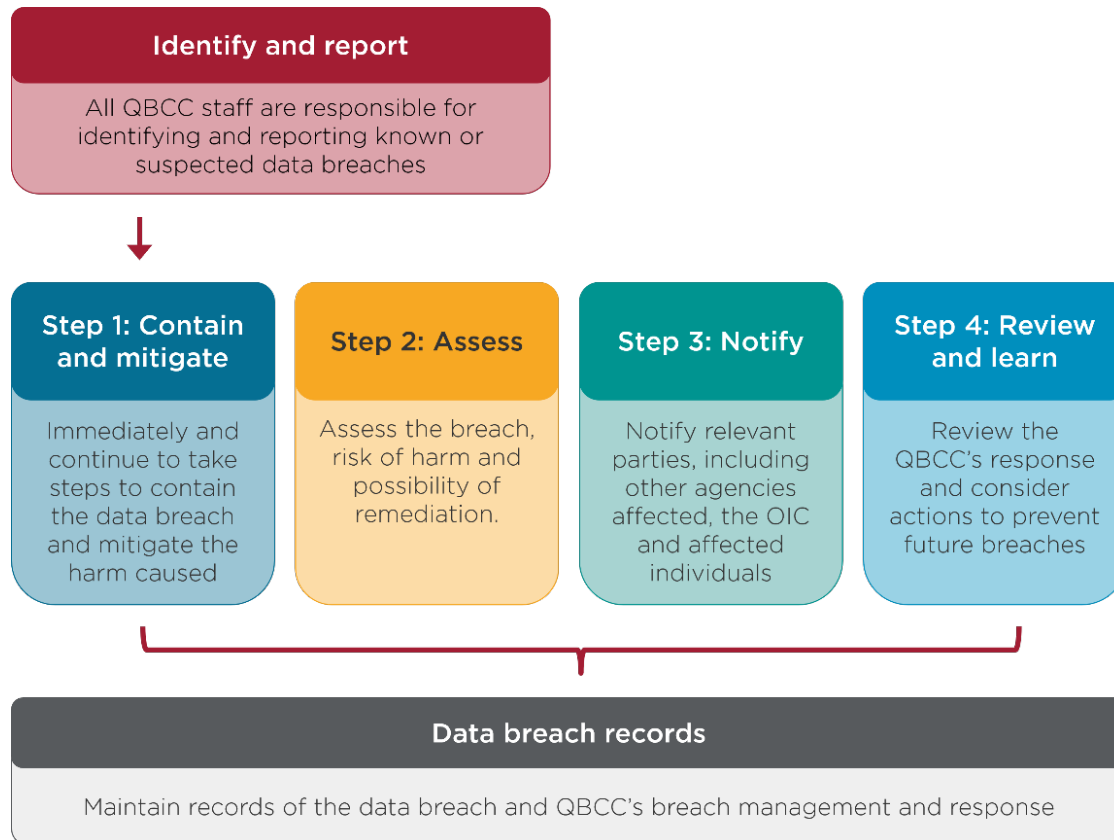
Affected individual	An individual to whom the personal information relates, and who is likely to suffer serious harm as a result of the data breach – see section 47(1)(a)(ii) of the IP Act.
Cyber incident	A cyber incident is an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.
Data breach	The unauthorised access to, or unauthorised disclosure of, information or the loss of information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur in accordance with schedule 5 of the IP Act.
Data Breach Response Plan	A Plan that assists the QBCC with meeting its legislative obligations in relation to managing eligible data breaches under the IP Act and that sets out how the QBCC manages and responds to an eligible data breach. The Data Breach Response Plan also outlines the composition of the Data Breach Response Team, including roles and responsibilities.
Data Breach Response Team	A cross-functional team that is activated to manage high-risk eligible data breaches and includes the senior manager (e.g., Senior Leadership Team member, Executive Director, or Director) from the following areas: <ul style="list-style-type: none"> <li>• Impacted business area</li> <li>• Legal and Legislation (includes Privacy)</li> <li>• Digital and Information</li> <li>• Human Resources</li> <li>• Integrity and Risk</li> <li>• Customer and Strategy</li> </ul>
Eligible data breach	An “Eligible Data Breach” will have occurred under section 47 of the IP Act where: <p>a) there has been unauthorised access to, or unauthorised disclosure of <b>personal information</b> held by an agency, <b>and</b></p> <p>the access or disclosure is likely to result in <b>serious harm</b> to any of the <b>individuals</b> to whom the information relates; <b>or</b></p> <p>b) there has been loss of <b>personal information</b> held by an agency that is likely to result in unauthorised access to, or unauthorised disclosure of the personal information, <b>and</b></p> <p>the loss is likely to result in <b>serious harm</b> to any of the <b>individuals</b> to whom the information relates.</p>
<i>Held or hold in relation to personal information</i>	Defined in section 13 of the IP Act as: <i>Personal information is <b>held</b> by a relevant entity, or the entity <b>holds</b> personal information, if the personal information is contained in a document in the possession, or under the control, of the relevant entity.</i>
Information Commissioner	The Queensland Information Commissioner
IP Act	<i>Information Privacy Act 2009 (QLD)</i>

<i>Likely to result</i>	The risk of serious harm to an individual whose personal information is involved in the breach is more probable than not, as opposed to it being merely possible.
MNDB scheme	The mandatory notification of data breach scheme provided under Chapter 3A of the IP Act, that imposes obligations on the QBCC to contain, mitigate and assess known or suspected eligible data breaches and notify the Information Commissioner and affected individuals.
Personal information	Personal Information is defined in section 12 of the IP Act as: <i>Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion –</i> a) <i>whether the information or opinion is true or not; and</i> b) <i>whether the information or opinion is recorded in a material form or not</i>
Privacy complaint	A complaint about the QBCC's collection, use, disclosure or storage of an individual's personal information.
Serious harm	Defined in schedule 5 of the IP Act as: <ul style="list-style-type: none"> <li>• <i>serious physical, psychological, emotional, or financial harm to the individual because of the access or disclosure; or</i></li> <li>• <i>serious harm to the individual's reputation because of the access or disclosure.</i></li> </ul> <p><b>Note:</b> the above definition is not exhaustive and there are other kinds of harm that can meet the 'serious' threshold. Serious harm occurs where the harm arising from the data breach has, or may, result in a real and substantial detrimental effect to an individual. The effect on an individual must be more than mere irritation, annoyance, or inconvenience.</p>
TFN	A tax file number (TFN) is a unique identifier issued by the Commissioner of Taxation to individuals and entities for tax administration purposes.

# APPENDIX B: DATA BREACH RESPONSE

The QBCC establishes and maintains a Data Breach Response Plan that outlines the steps followed in the event of a data breach. The figure below illustrates, at a high level, how a data breach is managed at the QBCC.

Figure 1: Data breach response steps



Making and maintaining records about eligible data breaches should also be done in accordance with the *Public Records Act 2023*. Additionally, all records containing personal information must be handled in accordance with the Queensland Privacy Principles set out in the *Information Privacy Act 2009*.